Surfer en toute sécurité sur le World Wide Web : les 10 commandements

1. Installez un antivirus et procédez régulièrement à un scan

Comme les programmes antivirus peuvent prendre un certain temps avant de reconnaître de nouveaux virus, ils passent parfois entre les mailles du filet. Veillez donc à toujours disposer de la dernière version du programme antivirus sur votre ordinateur et restez vigilant. N'oubliez pas non plus que, pour les versions gratuites des antivirus, les mises à jour ne sont pas toujours précises ni offertes à temps.

Vous recevez un document par e-mail ou vous voulez placer des fichiers sur votre ordinateur à partir d'une clé USB ? Scannez-les toujours avant de les ouvrir. Cette opération peut se faire simplement au moyen d'un antivirus.

Les virus peuvent se diffuser non seulement par e-mail ou lors de l'échange de fichiers, mais aussi lors d'une simple visite sur un site web inconnu ou trompeur, qui entraînera la contamination de votre ordinateur. Les exemples de sources de contamination les plus connues sont les sites de Torrent et sites porno.

Pour des organisations professionnelles, il est conseillé d'utiliser différents types de produits antivirus, afin d'augmenter la fréquence d'installation de nouvelles « signatures antivirus », par exemple toutes les 5 minutes.

Attention :

Lorsque vous visitez un site web, n'acceptez jamais une proposition ou une notification d'installation d'un antivirus ou d'autres produits logiciels. Cela mène souvent à l'installation de logiciels malveillants.

Quels risques limitez-vous ainsi ?

Vous contrôlez plus ou moins le risque de logiciels espions, de chevaux de Troie, etc. Vous limitez le risque de faire partie à votre insu d'un « botnet ». Dans le jargon, un ordinateur faisant partie d'un « botnet » est appelé « zombie ».

2. Tenez automatiquement à jour votre ordinateur et vos programmes

Vérifiez les paramètres de votre ordinateur, tablette et *smartphone*, et, si possible, activez la mise à jour automatique, ou procédez régulièrement vous-même aux mises à jour.

Une série de programmes (comme Adobe PDF Reader, Java, Flash Player, applications de l'App Store) et divers navigateurs (comme Internet Explorer, Firefox et Chrome) proposent également des mises à jour automatiques.

Quels risques limitez-vous ainsi ?

Vous limitez le risque que des pirates informatiques (« hackers ») ou « botnets » prennent le contrôle, en raison de faiblesses connues du logiciel, sur ce que vous faites avec votre ordinateur, *smartphone* ou tablette.

3. Effectuez régulièrement une copie de secours sur un disque dur externe

Effectuez régulièrement une copie de secours sur un ou plusieurs disque(s) dur(s) externe(s). Conservez-la en lieu sûr et ne l'**associez jamais** à votre ordinateur ou réseau. Vous limiterez ainsi les pertes de données précieuses en cas d'attaque d'un « ransomware » (logiciel de rançon). Ce type de logiciel malveillant permet aux *hackers* de faire chanter leurs victimes en cryptant tous les dossiers de leur PC et disques durs associés. Pour que les victimes récupèrent leurs documents, photos et tout ce qu'elles ont enregistré, les pirates informatiques demandent un paiement en « Bitcoins ». Il s'agit généralement d'un piège dans lequel il est préférable de ne pas tomber.

Quels risques limitez-vous ainsi ?

En cas de problèmes techniques ou lorsque votre ordinateur est attaqué par un « ransomware », vous pouvez vous appuyer sur une copie afin de ne pas perdre toutes vos données.

Pertes de données en général.

4. Méfiez-vous !

Restez toujours sur vos gardes lorsque l'on vous propose quelque chose de gratuit. Il peut s'agir d'une fenêtre contextuelle affichant une offre exceptionnelle qui vous invite à consulter des pages web, de courriels ou d'appels téléphoniques. Ne réagissez pas trop vite. Faites preuve de bon sens. Si vous connaissez l'expéditeur d'un message qui vous semble suspect, contactez cette personne pour vérifier si ce courriel provient bien d'elle.

Il suffit d'une visite sur un site web inconnu ou trompeur pour contaminer votre ordinateur. Les sites de Torrent et sites porno constituent des sources de contamination connues.

Méfiez-vous lorsque vous recevez un fichier attaché par e-mail, même d'une connaissance, ou lorsque vous recevez une clé USB par la poste. Si vous êtes inquiet, contactez l'expéditeur. Une clé USB peut en effet être contaminée avec un virus non reconnu par le logiciel antivirus. Cette pratique est appelée « spear phishing ». Pour ces mêmes raisons, soyez aussi prudent quand vous laissez traîner des clés USB.

Faites aussi attention à ce que vous publiez sur les réseaux sociaux et sur Internet. En effet, la « hacking community » utilise souvent, pour des attaques ciblées, des données qu'elle trouve sur Internet au sujet de certaines personnes. On appelle cette pratique le « social engineering ». Google est l'une des banques de données la plus utilisée par les pirates informatiques et elle est entièrement gratuite.

Pour prévenir des attaques ciblées, il convient donc de recourir à des moyens techniques (pare-feu, logiciels antivirus et autres outils). Bien que ces outils soient nécessaires, la façon de traiter l'information et de se comporter sur Internet ainsi que les informations mises inconsciemment à la

disposition de *hackers* jouent également un grand rôle. Au moyen des données que les pirates informatiques se procurent sur Internet à propos des personnes et/ou organisations, la « hacking community » utilise les informations pour tromper les systèmes de sécurité standard (antivirus, pare-feu, détection d'intrusion,...). Dans le jargon, cette technique est connue sous le nom de « social engineering » et a pour but ultime de tromper les gens et/ou d'infiltrer des organisations.

Quels risques limitez-vous ainsi ?

Vous limitez les risques de pertes de données, de virus, de programmes malveillants (« malware ») et d'espionnage.

5. N'installez des logiciels que s'ils proviennent d'une source fiable

Ne téléchargez jamais un programme sur le premier site web proposé par un moteur de recherche (tel que Google), mais optez toujours pour le site web officiel du développeur du programme.

Quels risques limitez-vous ainsi ?

Vous limitez les risques de pertes de données, de virus, de programmes malveillants (« malware ») et d'espionnage.

6. Choisissez des mots de passe sécurisés, ne les réutilisez pas, ne les partagez jamais et renouvelez-les régulièrement

La règle d'or : au plus le mot de passe est long et complexe, au mieux il est protégé.

Pour vous souvenir facilement d'un mot de passe, vous pouvez utiliser une longue phrase, qui est en outre plus sûre qu'un simple mot.

Vous pouvez également recourir à des programmes spéciaux, baptisés « coffres-forts à mots de passe », qui créeront et se souviendront du mot de passe pour vous.

Renouvelez régulièrement vos mots de passe. Lorsque vous vous enregistrez sur des sites web, utilisez toujours des mots de passe et adresses e-mail différents.

Outre votre mot de passe, on peut également vous demander d'introduire un code qui vous est envoyé directement sur votre GSM personnel. Vous pouvez souvent activer vous-même cette fonctionnalité dans le programme ou sur le site web que vous utilisez.

Il est facile de deviner les réponses aux questions secrètes que vous pouvez choisir pour mieux protéger ou réinitialiser votre mot de passe. Si vous devez néanmoins le faire, le mieux est de ne pas répondre à la question mais de donner une réponse fictive. Veillez toutefois à bien vous souvenir de votre réponse ou à utiliser un coffre-fort à mots de passe.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact en cas d'abus de votre compte. En effet, si vos mots de passe et comptes ont été piratés sur le Net, il sera plus difficile pour les « hackers » de les réutiliser.

7. Surfez via https pour éviter que la communication ne soit interceptée

Lorsque https:// est indiqué dans votre navigateur au début d'un site que vous voulez visiter, cela signifie que la connexion est sécurisée. Si un message d'erreur apparaît pour vous informer que le certificat n'est pas correct, cette connexion n'est plus sécurisée.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et l'interception de la communication.

8. Sécurisez votre réseau Wi-Fi à domicile

Sécurisez votre réseau à domicile avec un mot de passe.

Ainsi, vous empêcherez aussi bien les cybercriminels que vos voisins d'utiliser votre connexion Internet sans fil.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et l'interception de la communication.

9. Veillez à ce que la mémoire de votre appareil soit totalement effacée lorsque vous ne souhaitez plus l'utiliser

Vous pouvez vider la mémoire de votre *smartphone* ou tablette via l'option « Effacer » de votre appareil. Il vaut mieux effacer complètement (formater) votre ordinateur fixe ou portable. Un formatage rapide n'est pas une bonne idée car il reste toujours des données. Faites-vous éventuellement assister d'un expert informatique pour procéder à un formatage approfondi.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et empêchez que des noms d'utilisateur et mots de passe tombent dans de mauvaises mains.

10. Soyez vigilant quand vous utilisez du Wi-Fi public

N'introduisez pas de mots de passe pour des comptes importants – tels qu'un e-mail ou un paiement en ligne – lorsque vous travaillez sur un réseau sans fil non sécurisé.

Quels risques limitez-vous ainsi ?

Vous limitez l'impact des pertes de données et l'interception de la communication.

Sources

(https://www.safeonweb.be/nl/tips)

(https://cert.europa.eu/cert/alertedition/en/malware.html)

(https://pentestmag.com/the-cyberwar)